Middlesex University London

# Middlesex University Research Repository

An open access repository of

Middlesex University research

http://eprints.mdx.ac.uk

Elmer, Jonathan ORCID logoORCID: https://orcid.org/0000-0001-5296-1987 and Kohls, Martin (2017) On separating a fixed point from zero by invariants. Communications in Algebra, 45 (1) . pp. 371-375. ISSN 0092-7872 [Article] (doi:10.1080/00927872.2016.1175465)

Final accepted version (with author's formatting)

This version is available at: https://eprints.mdx.ac.uk/20905/

**Copyright:**

Middlesex University Research Repository makes the University's research available electronically.

Copyright and moral rights to this work are retained by the author and/or other copyright owners unless otherwise stated. The work is supplied on the understanding that any use for commercial gain is strictly forbidden. A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge.

Works, including theses and research projects, may not be reproduced in any format or medium, or extensive quotations taken from them, or their content changed in any way, without first obtaining permission in writing from the copyright holder(s). They may not be sold or exploited commercially in any format or medium without the prior written permission of the copyright holder(s).

Full bibliographic details must be given when referring to, or quoting from full items including the author's name, the title of the work, publication details where relevant (place, publisher, date), pagination, and for theses or dissertations the awarding institution, the degree type awarded, and the date of the award.

If you believe that any material held in the repository infringes copyright law, please contact the Repository Team at Middlesex University via the following email address:

eprints@mdx.ac.uk

The item will be removed from the repository while any claim is being investigated.

See also repository copyright: re-use policy: http://eprints.mdx.ac.uk/policies.html#copy

# ON SEPARATING A FIXED POINT FROM ZERO BY INVARIANTS

JONATHAN ELMER AND MARTIN KOHLS

Abstract. Assume a fixed point $v \in V^G$ can be separated from zero by a homogeneous invariant $f \in \Bbbk[V]^G$ of degree $p^r d$ where $p > 0$ is the characteristic of the ground field $\Bbbk$ and $p, d$ are coprime. We show that then $v$ can also be separated from zero by an invariant of degree $p^r$, which we obtain explicitly from $f$. It follows that the minimal degree of a homogeneous invariant separating $v$ from zero is a $p$-power.

## 1. Introduction

Let $G$ be a linear algebraic group over an infinite field $\Bbbk$ of any characteristic and let $X$ be an algebraic variety over $\Bbbk$ on which $G$ acts. Then $G$ acts naturally on the ring of functions $\Bbbk[X]$ by $g(f) := f \circ g^{-1}$ for $f \in \Bbbk[X]$ and $g \in G$. The ring of fixed points of this action is denoted by $\Bbbk[X]^G$ and we call this the ring of invariants. If $G$ acts linearly and rationally on a finite dimensional $\Bbbk$-vector space $V$ then we call $V$ a $G$-module, and $\Bbbk[V]$ is the set of polynomial functions $V \to \Bbbk$. In that case we have a natural grading $\Bbbk[V] = \oplus_{d=0}^{\infty} \Bbbk[V]_d$ by total degree which is preserved by the action of $G$, and we have $\Bbbk[V] = S(V^*)$, the symmetric algebra of the dual of $V$. Determining whether the ring of invariants $\Bbbk[X]^G$ is finitely generated is one of the oldest and most difficult problems in invariant theory. Hilbert was able to prove finite generation in the case where $G = \mathrm{SL}_n$ or $\mathrm{GL}_n$ and $\Bbbk$ a field of characteristic zero. Hilbert's argument can be extended to any group with the following property: for every $G$-module $V$, and every nonzero fixed point $v \in V^G$ there exists an invariant linear function $f \in (V^*)^G$ such that $f(v) \neq 0$. Such groups are called *linearly reductive*. Linear reductivity of $G$ is equivalent to the condition that all representations of $G$ over $\Bbbk$ are completely reducible. Nagata made a major breakthrough by considering a more general class of groups. We say that $G$ is *geometrically reductive* if the following property holds: for every $G$-module $V$ and every nonzero fixed point $v \in V^G$ there exists a homogeneous invariant function $f \in \Bbbk[V]^G$ of positive degree such that $f(v) \neq 0$. Nagata [8] was able to prove that if $G$ is geometrically reductive then $\Bbbk[X]^G$ is finitely generated for all $X$. Nagata and Miyata [9] subsequently showed that a geometrically reductive group must be reductive, a purely group-theoretic condition on $G$. It was conjectured by Mumford [7] that all reductive groups are geometrically reductive, a fact finally proved by Haboush [5] several years later. Now let $G$ be a linear algebraic group over $\Bbbk$ and let $V$ be a $G$-module. Following [3] we define for any $v \in V$

$$\epsilon(G, v) := \inf\{d \in \mathbb{N}_{>0} \mid \text{ there exists } f \in \Bbbk[V]^G_d \text{ such that } f(v) \neq 0\},$$

where the infimum of an empty set is infinity. Thus, $G$ is reductive if $\epsilon(G, v)$ is finite for all nonzero $v \in V^G$ and linearly reductive if $\epsilon(G, v) = 1$ for all nonzero $v \in V^G$. Nagata and Miyata [9, Proof of Theorem 1] also proved that if $v \in V^G$

*Date*: December 7, 2015.

2010 *Mathematics Subject Classification.* 13A50.

*Key words and phrases.* Invariant theory, linear algebraic groups, geometrically reductive, prime characteristic.

and there exists $f \in \Bbbk[V]^G_d$ such that $f(v) \neq 0$ with $d$ invertible in $\Bbbk$, then there exists $\tilde{f} \in \Bbbk[V]^G_1$ such that $f(v) \neq 0$. Consequently for any nonzero $v \in V^G$, $\epsilon(G, v)$ is equal to one, divisible by $p = \mathrm{char}(\Bbbk)$ or infinite. In particular, if $\mathrm{char}(\Bbbk) = 0$ then every (geometrically) reductive group over $\Bbbk$ is linearly reductive. A version of their argument rephrased in language consistent with this note can be found in [3, Proposition 2.1]. The main purpose of this article is to prove the following result generalising the above in the case of positive characteristic:

**Theorem 1.1.** *Let $p = \mathrm{char}(\Bbbk) \geq 0$, $r \geq 0$ an integer and $d \geq 1$ an integer invertible in $\Bbbk$. Let $v \in V^G \setminus \{0\}$ be a nonzero fixed point and suppose there exists a homogeneous invariant $f$ of degree $p^r d$ such that $f(v) \neq 0$. Then there exists a homogeneous invariant $\tilde{f}$ of degree $p^r$ such that $\tilde{f}(v) \neq 0$. In particular, for any $v \in V^G$ we have that $\epsilon(G, v)$ is either a power of $p$ (including $p^0 = 1$) or $\infty$.*

One says that a pair of points $v, w \in V$ can be *separated* if there exists an invariant $f \in \Bbbk[V]^G$ such that $f(v) \neq f(w)$. It has become quite popular recently to investigate so called *separating sets*, which are subsets $S$ of the invariant ring with the following property: whenever two points can be separated, then they can be separated by an element of $S$. This research topic was introduced by Derksen and Kemper [1, Definition 2.3.8], and quite a number of papers have appeared which deal with this topic. Remarkably, it turns out that even if the ring of invariants $\Bbbk[V]^G$ is not finitely generated, it still contains a finite separating set, see [1, Theorem 2.3.15]. From the point of view of this research topic, we deal with separating a fixed point $v \in V^G$ from the zero point $w = 0$. Recall that, for any $G$ and $V$, *Hilbert's Nullcone* $\mathcal{N}_{G,V}$ is defined to be the vanishing set of all homogeneous invariants of positive degree. It is natural to consider the quantity

$$\delta(G, V) := \sup\left(\{\epsilon(G, v) \mid v \in V^G \setminus \mathcal{N}_{G,V}\} \cup \{0\}\right).$$

Since a separating set must certainly contain an invariant separating a given point outside the nullcone from zero, [1, Theorem 2.3.15] implies that $\delta(G, V)$ is finite for any $G$ and $V$. If $G$ is linearly reductive then $\delta(G, V) \leq 1$ for all $V$. For this reason, the number $\delta(G, V)$ can be considered as a measure for the *"degree of reductivity"* of the representation $V$. Further results on $\delta(G, V)$ can be found in [2], [3] and [6]. Our main theorem implies immediately

**Corollary 1.2.** *For any $G$-module $V$, we have that $\delta(G, V)$ is zero, one, or a power of $p = \mathrm{char}(\Bbbk)$.*

This article is organised as follows: in section two we prove Theorem 1.1. In section three we give an example showing how the theorem may be used to compute $\delta(G, V)$ in cases where the ring of invariants is difficult to compute.

## 2. Separating fixed points from zero

Before we prove our main result, we want to reproduce the argument showing that in positive characteristic $p$, given a reductive group $G$ and a nonzero fixed point $v \in V^G$, there exists an invariant of $p$-power degree separating $v$ from zero. This is a consequence of the following standard result for reductive groups.

**Theorem 2.1** (see [7, Lemma A1.2])**.** *Let $G$ be a reductive group over a field of positive characteristic $p$ and $V, W$ be $G$-modules. If $\phi : \Bbbk[V] \to \Bbbk[W]$ is a surjective $G$-equivariant algebra-homomorphism, then for any $f \in \Bbbk[W]^G$ there exists an $r \geq 0$ such that $f^{p^r} \in \phi(\Bbbk[V]^G)$.*

Now consider $v \in V^G \setminus \{0\}$. We define $W := \Bbbk v$ and write $\Bbbk[W] = \Bbbk[x]$. The restriction map $\phi : \Bbbk[V] \to \Bbbk[W]$, $f \mapsto f|_W$ is clearly surjective and $G$-equivariant, and as $x \in \Bbbk[W]^G$ the theorem implies the existence of an invariant $f \in \Bbbk[V]^G$ such

that $f|_W = x^{p^r}$ for some $r \geq 0$. It follows that for $h$ the degree $p^r$-component of $f$, we also have $h|_W = x^{p^r}$, and $h$ is a homogeneous invariant of degree $p^r$ satisfying $h(v) = h|_W(v) = x^{p^r}(v) = 1 \neq 0$.

Note that although this result implies that every nonzero fixed point $v$ can be separated from zero by an invariant of $p$-power degree, it does not imply that the minimal possible degree of an invariant separating $v$ from zero is also a $p$-power. This is a consequence of Theorem 1.1 which we prove now. The proof is based on similar ideas to those used by Nagata and Miyata; indeed, it specialises to their proof in the case $r = 0$.

*Proof of Theorem 1.1.* We extend $v_0 := v$ to a basis $\{v_0, v_1, \ldots, v_n\}$ of $V$ and form the corresponding dual basis $\{x_0, x_1, \ldots, x_n\}$ of $V^*$. Then $f$ has the form $f = \sum_{i=0}^{p^r d} x_0^{p^r d - i} c_i$, where $c_i \in \Bbbk[x_1, \ldots, x_n]_i$ and $f(v_0) = c_0 \in \Bbbk \setminus \{0\}$. Dividing by $c_0$, we may assume $c_0 = 1$. We claim that

$$\tilde{f} := x_0^{p^r} + \frac{1}{d} \sum_{i=1}^{p^r} x_0^{p^r - i} c_i$$

has the properties we require. Clearly, $\tilde{f}(v_0) = 1 \neq 0$, and $\tilde{f}$ is homogeneous of degree $p^r$. It remains to show that $\tilde{f}$ is invariant. We will obtain $\tilde{f}$ as the image of $f$ under a $G$-equivariant map $\Bbbk[V]_{p^r d} \to \Bbbk[V]_{p^r}$. We have $V^* = \Bbbk[x_1, \ldots, x_n]_1 \oplus \Bbbk x_0$ as vector spaces. Since $v_0 \in V^G$, we have that $\Bbbk[x_1, \ldots, x_n]_1$ is a $G$-submodule of $V^*$. Consider the $G$-module $\Bbbk[x_0, \ldots, x_n]_{p^r d}$ and the subspace

$$T := \bigoplus_{i=p^r+1}^{p^r d} \Bbbk[x_0]_{p^r d - i} \otimes \Bbbk[x_1, \ldots, x_n]_i,$$

i.e. the set of polynomials of $\Bbbk[x_0, \ldots, x_n]_{p^r d}$ which have total degree at least $p^r + 1$ in the variables $x_1, \ldots, x_n$. As $v_0 \in V^G$ we have, for any $g \in G$,

$$g(x_0) = x_0 + \gamma(g) \qquad \text{for some} \quad \gamma(g) \in \Bbbk[x_1, \ldots, x_n]_1.$$

It follows that $T$ is in fact a $G$-submodule of $\Bbbk[x_0, \ldots, x_n]_{p^r d}$. We next show that the map

$$\phi : \Bbbk[x_0, \ldots, x_n]_{p^r d}/T \mapsto \Bbbk[x_0, \ldots, x_n]_{p^r}$$

given by $\Bbbk$-linear extension of

$$\begin{aligned} x_0^{p^r d} + T &\mapsto x_0^{p^r} \\ x_0^{p^r d - k} b_k + T &\mapsto \tfrac{1}{d} x_0^{p^r - k} b_k \qquad \text{for } b_k \in \Bbbk[x_1, \ldots, x_n]_k \text{ and } k = 1, \ldots, p^r \end{aligned}$$

is an isomorphism of $G$-modules. Clearly $\phi$ is an isomorphism of $\Bbbk$-vector spaces, so it remains to show that $\phi$ is $G$-equivariant, i.e. $\phi(g(m + T)) = g(\phi(m + T))$ for every $g \in G$ and $m \in \Bbbk[x_0, \ldots, x_n]_{p^r d}$. By $\Bbbk$-linearity, it is enough to consider the cases $m = x_0^{p^r d}$ and $m = x_0^{p^r d - k} b_k$ for $b_k \in \Bbbk[x_1, \ldots, x_n]_k$ and $k = 1, \ldots, p^r$. Assume $m = x_0^{p^r d}$ first. We fix $g \in G$, set $\gamma := \gamma(g)$ and compute

$$\phi(g(x_0^{p^r d} + T)) = \phi((x_0 + \gamma)^{p^r d} + T) = \phi((x_0^{p^r} + \gamma^{p^r})^d + T) \overset{(*)}{=}$$
$$\phi(x_0^{p^r d} + d x_0^{p^r (d-1)} \gamma^{p^r} + T) = x_0^{p^r} + \gamma^{p^r} = (x_0 + \gamma)^{p^r} =$$
$$g(x_0^{p^r}) = g(\phi(x_0^{p^r d} + T)).$$

Note that in (*) we have used that $x_0^{p^r (d-j)} \gamma^{p^r j} \in T$ for $j \geq 2$. Secondly assume $m = x_0^{p^r d - k} b_k$ with $1 \leq k \leq p^r$ and $b_k \in \Bbbk[x_1, \ldots, x_n]_k$. We write $\widetilde{b_k} := g(b_k) \in \Bbbk[x_1, \ldots, x_n]_k$. In the following computation we will use that $\binom{p^r d - k}{j} \equiv \binom{p^r - k}{j}$ mod $p$ for $k = 1, \ldots, p^r$ and $j = 0, \ldots, p^r - k$, see Lemma 2.2 below. We obtain

$$\phi(g(x_0^{p^r d - k} b_k + T)) = \phi((x_0 + \gamma)^{p^r d - k} \widetilde{b_k} + T) =$$

$$\phi\left(\sum_{j=0}^{p^rd-k}\binom{p^rd-k}{j}x_0^{p^rd-k-j}\gamma^j\widetilde{b_k}+T\right).$$

Note that $\gamma^j\widetilde{b_k}\in\Bbbk[x_1,\dots,x_n]_{j+k}$. In particular, for $j\geq p^r+1-k$, we have $x_0^{p^rd-k-j}\gamma^j\widetilde{b_k}\in T$, so in the sum above only summands for $j=0,\dots,p^r-k$ have to be taken into account. Also note that $k\geq 1$, so each term of $\gamma^j\widetilde{b_k}$ is of positive degree. Now by the definition of $\phi$ we obtain

$$\phi(g(x_0^{p^rd-k}b_k+T))=\phi\left(\sum_{j=0}^{p^r-k}\binom{p^rd-k}{j}x_0^{p^rd-k-j}\gamma^j\widetilde{b_k}+T\right)=$$

$$\sum_{j=0}^{p^r-k}\binom{p^rd-k}{j}\frac{1}{d}x_0^{p^r-k-j}\gamma^j\widetilde{b_k}\overset{\text{Lemma 2.2}}{=}\frac{1}{d}\sum_{j=0}^{p^r-k}\binom{p^r-k}{j}x_0^{p^r-k-j}\gamma^j\widetilde{b_k}=$$

$$\frac{1}{d}(x_0+\gamma)^{p^r-k}\widetilde{b_k}=g(\frac{1}{d}x_0^{p^r-k}b_k)=g(\phi(x_0^{p^rd-k}b_k+T)).$$

This shows that $\phi$ is indeed $G$-equivariant. Now let

$$\pi:\Bbbk[x_0,\dots,x_n]_{p^rd}\to\Bbbk[x_0,\dots,x_n]_{p^rd}/T$$

denote the canonical projection, which is $G$-equivariant as $T$ is a $G$-submodule. Then $\phi\circ\pi:\Bbbk[x_0,\dots,x_n]_{p^rd}\to\Bbbk[x_0,\dots,x_n]_{p^r}$ is a $G$-equivariant map, and hence it maps the invariant $f$ to the invariant

$$\phi(\pi(f))=\phi\left(\pi(\sum_{i=0}^{p^rd}x_0^{p^rd-i}c_i)\right)=\phi\left(\sum_{i=0}^{p^rd}x_0^{p^rd-i}c_i+T\right).$$

As for $i\geq p^r+1$ we have $x_0^{p^rd-i}c_i\in T$, only the summands where $i=0,\dots,p^r$ need to be considered, so we obtain

$$\phi(\pi(f))=\phi\left(\sum_{i=0}^{p^r}x_0^{p^rd-i}c_i+T\right)=\phi(x_0^{p^rd}+T)+\sum_{i=1}^{p^r}\phi(x_0^{p^rd-i}c_i+T)=$$

$$x_0^{p^r}+\frac{1}{d}\sum_{i=1}^{p^r}x_0^{p^r-i}c_i=\tilde{f}.$$

Hence, $\tilde{f}$ is $G$-invariant. □

We have used the following characteristic $p$-relation on binomial coefficients:

**Lemma 2.2.** *Assume $p$ is a prime and $d\geq 1$. Then we have*

$$\binom{p^rd-k}{j}\equiv\binom{p^r-k}{j}\mod p\qquad\text{for } k=1,\dots,p^r \text{ and } j=0,\dots,p^r-k.$$

*Proof.* We first recall the well known Theorem of Lucas on binomial coefficients modulo a prime (see [4] for a short proof): if $a,b$ are integers with $p$-adic expansions $a=\sum_{i=0}^\infty a_ip^i$ and $b=\sum_{i=0}^\infty b_ip^i$, then

$$\binom{a}{b}\equiv\prod_{i=0}^\infty\binom{a_i}{b_i}\mod p.$$

Of course, here almost all summands are zero and almost all factors are equal to 1, as $\binom{m}{0}=1$ for all $m\geq 0$. We now consider the base-$p$-expansions $j=\sum_{i=0}^\infty j_ip^i$, $p^rd-k=\sum_{i=0}^\infty a_ip^i$ and $p^r-k=\sum_{i=0}^\infty b_ip^i$, where all $j_i,a_i,b_i$ are zero for large enough $i$, and $0\leq j_i,a_i,b_i<p$ for all $i$. As $k\geq 1$ and $j\leq p^r-k$, we have that

$j_i = 0$ for $i \geq r$. As $p^r d - k = p^r - k + (d-1)p^r$, it follows that $a_i = b_i$ for $0 \leq i < r$. We thus have by Lucas' Theorem

$$\binom{p^r d - k}{j} \equiv \prod_{i=0}^{\infty} \binom{a_i}{j_i} \equiv \prod_{i=0}^{r-1} \binom{a_i}{j_i} \equiv \prod_{i=0}^{r-1} \binom{b_i}{j_i} \equiv \prod_{i=0}^{\infty} \binom{b_i}{j_i} \equiv \binom{p^r - k}{j} \mod p.$$

□

## 3. An example

Corollary 1.2 sometimes allows a determination of $\delta(G, V)$ for a given representation $V$ without knowledge of the invariant ring. The special case $p = 2$ of the following example was treated in [6, Proposition 12].

*Example* 3.1. Consider a field of positive characteristic $p$, the cyclic group $Z_p$ of order $p$, and the action of the group $G = Z_p \times Z_p = \langle g_1, g_2 \rangle$ on a $G$-module $V = \langle h_1, \ldots, h_m, e_1, \ldots, e_m \rangle$, $m \geq 2$, where $g_1$ acts by the matrix $\begin{pmatrix} I_m & 0 \\ I_m & I_m \end{pmatrix}$, and $g_2$ acts by the matrix $\begin{pmatrix} I_m & 0 \\ J_m(\lambda) & I_m \end{pmatrix}$. Here, $I_m$ denotes the $m \times m$ identity matrix, and $J_m(\lambda)$ a lower triangular $m \times m$ Jordan block with eigenvalue $\lambda \in \Bbbk$. Then $e_m \in V^G$, and we want to show that $\epsilon(G, e_m) = p^2$. Note that, since for a finite group we have $\delta(G, V) \leq |G|$ (see [2, Theorem 1.1]), this shows that $\delta(G, V) = p^2$.

We write $\Bbbk[V] = \Bbbk[x_1, \ldots, x_m, y_1, \ldots, y_m]$. We then have

$$\begin{array}{lcll} g_i(x_j) & = & x_j & \text{for } i = 1, 2,\ j = 1, \ldots, m \\ g_1(y_j) & = & y_j - x_j & \text{for } j = 1, \ldots, m \\ g_2(y_1) & = & y_1 - x_1 & \\ g_2(y_j) & = & y_j - \lambda x_j - x_{j-1} & \text{for } j = 2, \ldots, m. \end{array}$$

It is easy to see that $\Bbbk[V]_1^G = \langle x_1, \ldots, x_m \rangle$, which shows $\epsilon(G, e_m) > 1$. As $\epsilon(G, e_m)$ is a $p$-power by Theorem 1.1, and bounded above by $|G| = p^2$, it suffices to show that $\epsilon(G, e_m) \neq p$. To this end, we will demonstrate that $y_m^p$ does not appear in any invariant polynomial. Define

$$\Delta_{i,j} : \Bbbk[V] \to \Bbbk[V], \quad f \mapsto g_1^i g_2^j(f) - f \qquad \text{for } i, j \in \mathbb{Z}.$$

Then for an invariant polynomial $f$, $\Delta_{i,j}(f) = 0$ for all $i, j$. We will say that a monomial $r$ *lies over* a monomial $s$ with respect to $\Delta_{i,j}$ if $s$ appears in $\Delta_{i,j}(r)$. As $g_1^i g_2^j$ acts by the matrix $\begin{pmatrix} I_m & -iI_m - jJ_m(\lambda)^T \\ 0 & I_m \end{pmatrix}$ on $V^*$, it follows that if a monomial $r$ lies over $x_m^p$ with respect to $\Delta_{i,j}$ for some $i, j$, then $r$ is an element of the set $M := \{y_m^p, x_m y_m^{p-1}, x_m^2 y_m^{p-2}, \ldots, x_m^{p-1} y_m\}$. Let now $f \in \Bbbk[V]^G$ be an invariant. Let $h = \sum_{k=1}^{p} c_k y_m^k x_m^{p-k}$, $c_k \in \Bbbk$, be the partial sum of terms of $f$ with monomials from $M$. Then for all $i, j$, the coefficients of $x_m^p$ in $\Delta_{i,j}(f)$ (which is zero) and $\Delta_{i,j}(h)$ respectively are equal. From

$$\begin{aligned} \Delta_{-i,-1}(h) &= \Delta_{-i,-1}\left(\sum_{k=1}^{p} c_k y_m^k x_m^{p-k}\right) \\ &= \sum_{k=1}^{p} (c_k (y_m + (\lambda + i)x_m + x_{m-1})^k x_m^{p-k} - c_k y_m^k x_m^{p-k}) \\ &= \ldots + \sum_{k=1}^{p} c_k (\lambda + i)^k x_m^p + \ldots \end{aligned}$$

it follows that $\sum_{k=1}^{p} c_k (\lambda + i)^k = 0$ for $i = 0, \ldots, p-1$. Therefore all elements of the set $Z := \{\lambda, \lambda + 1, \ldots, \lambda + p - 1\}$ of size $p$ are roots of the polynomial

$q := \sum_{k=1}^{p} c_k X^k$. Clearly, 0 is also a root of $q$. Assume first $0 \notin Z$. Then the polynomial $q$ of degree $\leq p$ has the elements of $\{0\} \cup Z$ as $p+1$ different roots, i.e. $q = 0$. In particular, $c_p = 0$, which shows that $y_m^p$ does not appear in $f$, which we wanted to prove and we are done. Secondly assume $0 \in Z$. It follows $\lambda + i_0 = 0$ for some $i_0 \in \{0, \dots, p-1\}$, which implies $Z = \{0, 1, 2, \dots, p-1\}$. As $Z$ is also the set of roots of $X^p - X$, it follows $q = c(X^p - X)$ for some $c \in \Bbbk$, i.e. $c_p = c$, $c_1 = -c$, and the other $c_i$'s are zero. Therefore we have $h = c(y_m^p - x_m^{p-1} y_m)$. As $i_0 + \lambda = 0$, $g_1^{-i_0} g_2^{-1}$ acts by the matrix $\begin{pmatrix} I_m & i_0 I_m + J_m(\lambda)^T \\ 0 & I_m \end{pmatrix} = \begin{pmatrix} I_m & J_m(0)^T \\ 0 & I_m \end{pmatrix}$ on $V^*$. From this it can be seen that $x_m^{p-1} y_m$ is the only monomial that lies over $x_m^{p-1} x_{m-1}$ with respect to $\Delta_{-i_0,-1}$. Therefore, the coefficients of $x_m^{p-1} x_{m-1}$ in $\Delta_{-i_0,-1}(f)$ (which is zero) and

$$\Delta_{-i_0,-1}(-c x_m^{p-1} y_m) = -c x_m^{p-1}(y_m + x_{m-1}) + c x_m^{p-1} y_m = -c x_m^{p-1} x_{m-1}$$

are equal, hence $0 = c = c_p$. This shows that $y_m^p$ does not appear in $f$ as claimed.

*Remark* 3.2. In the above, it was easy to see that $p^2 \geq \epsilon(G, e_m) > 1$, and we showed $\epsilon(G, e_m) \neq p$. Theorem 1.1 allowed us to conclude that $\epsilon(G, e_m) = p^2$. If $p = 2$ this follows straight away from Nagata and Miyata's result, but if $p > 2$ it is hard to rule out the possibility that $\epsilon(G, e_m) = dp$ for some $1 < d < p$ without using our theorem.

**Acknowledgments.** This paper was prepared during a visit of the first author to TU München. We want to thank Gregor Kemper for making this visit possible.

## References

[1] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[2] Jonathan Elmer and Martin Kohls. Zero-separating invariants for finite groups. *J. Algebra*, 411:92–113, 2014.

[3] Jonathan Elmer and Martin Kohls. Zero-separating invariants for linear algebraic groups. *To appear in Proceedings of the Edinburgh Mathematical Society*, 2015.

[4] N. J. Fine. Binomial coefficients modulo a prime. *Amer. Math. Monthly*, 54:589–592, 1947.

[5] W. J. Haboush. Reductive groups are geometrically reductive. *Ann. of Math. (2)*, 102(1):67–83, 1975.

[6] Martin Kohls and Müfit Sezer. Degree of reductivity of a modular representation. *available from arXiv:1406.6299*, 2014.

[7] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2)*. Springer-Verlag, Berlin, third edition, 1994.

[8] Masayoshi Nagata. Invariants of a group in an affine ring. *J. Math. Kyoto Univ.*, 3:369–377, 1963/1964.

[9] Masayoshi Nagata and Takehiko Miyata. Note on semi-reductive groups. *J. Math. Kyoto Univ.*, 3:379–382, 1963/1964.

University of Aberdeen, King's College, Aberdeen, AB24 3UE
*E-mail address*: j.elmer@abdn.ac.uk

Technische Universität München, Zentrum Mathematik-M11, Boltzmannstrasse 3, 85748 Garching, Germany
*E-mail address*: kohls@ma.tum.de